

**ORIGINAL**

Before the  
**FEDERAL COMMUNICATIONS COMMISSION**  
Washington, D.C. 20554

**In the Matter of:**

**Communications Assistance for  
Law Enforcement Act**

**CC Docket No. 97-213  
FCC No. 98-282**

**RECEIVED**

DEC 14 1998

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

**COMMENTS OF THE  
TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

Stewart A. Baker  
Thomas M. Barba  
L. Benjamin Ederington  
Steptoe & Johnson LLP  
1330 Connecticut Avenue, N.W.  
Washington, D.C. 20036  
(202) 429-3000

Grant Seiffert  
Vice President, Government Relations  
Matthew J. Flanigan  
President  
**Telecommunications Industry Association**  
1300 Pennsylvania Avenue, N.W.  
Suite 350  
Washington, DC 20004  
(202) 383-1483

No. of Copies rec'd 075  
List ABCDE

## SUMMARY

In early 1995, the telecommunications industry -- working through the Telecommunications Industry Association's ("TIA") Engineering Subcommittee TR 45.2 -- began the difficult task of building a standard to implement the Communications Assistance for Law Enforcement Act ("CALEA"). In developing this standard, Subcommittee TR 45.2 carefully balanced the competing interests of public safety, individual privacy and technological innovation. The Subcommittee also worked in close consultation with representatives of law enforcement, privacy organizations, and other industry associations and standards-setting bodies. The result, as the Commission notes, is a technical standard for the cellular, wireline and broadband PCS industries (J-STD-025) that enjoys almost universal approval.

Indeed, out of all of the features and provisions contained in this voluminous standard, only eleven proposed modifications are at issue in this proceeding. And even the parties who proposed these modifications strongly disagree in their criticisms of the standard. For example, although the Department of Justice and the Federal Bureau of Investigation ("FBI") argue that J-STD-025 should incorporate nine additional features (the "punch list"), they agree with industry that the two modifications proposed by the Center for Democracy and Technology ("CDT") are unnecessary. Similarly, although CDT suggests that J-STD-025's treatment of location and packet-mode communications should be modified, it strongly opposes the inclusion of the FBI's punch list.

TIA respectfully submits that the record in this proceeding clearly establishes that J-STD-025 is not deficient and, hence, that none of the proposed modifications to the standard are required by CALEA. TIA urges the Commission to reach the same conclusion.

Indeed, the Commission already has tentatively determined that four of the proposed modifications are not necessary. TIA endorses these conclusions. Specifically, TIA agrees that location information, as provided by J-STD-025 (i.e., “cell site location at the beginning and termination of the call”), is consistent with the requirements of Section 103 of CALEA. TIA also agrees with the Commission that at least three of the FBI’s punch list items (surveillance status message, continuity check tone, and feature status message) exceed the scope of CALEA.

As for the other seven items on which the Commission has not yet reached a formal conclusion, TIA believes that the Commission should eventually decide that these proposed modifications also are not required. J-STD-025 already provides, in the most cost-efficient manner, that information that is required by CALEA and is “reasonably available” to carriers. TIA believes that the Commission should conclude (as Subcommittee TR 45.2 did) that these proposed modifications are neither: i) required by Section 103, ii) reasonably available, nor iii) consistent with the five factors outlined by Congress in Section 107(b) for the Commission’s consideration.

The proposed modification to J-STD-025’s treatment of packet-mode communications is of special concern to TIA’s members. As the Commission is aware, the telecommunications network is rapidly evolving toward a packet-based architecture. It is imperative that the Commission not stifle the continued development of packet-mode technologies by imposing a solution that could require the redesign (or even abandonment) of certain technologies. Accordingly, TIA strongly urges the Commission to preserve the flexible approach contained in J-STD-025.

Whatever decision the Commission reaches on these eleven items, TIA agrees with the Commission's proposed method for implementing its eventual Report and Order. TIA respectfully urges that the Commission -- pursuant to its authority under Section 107(b)(5) -- establish a transition period of no less than 36 months from June 30, 2000 (the Commission's deadline for the "core" J-STD-025) for carriers to comply with the Commission's decision. This transition period would provide manufacturers approximately 24 months to design and develop the software and hardware modifications necessary to implement the Commission's order and would provide carriers roughly another 12 months to install and test these modifications.

TIA also endorses the Commission's conclusion to authorize Subcommittee TR 45.2 to revise J-STD-025, consistent with the requirements the Commission ultimately adopts in this proceeding. Because of its unique expertise and resources, TR 45.2 is best qualified to issue such a technical standard in the most efficient and expeditious manner. TIA will make every effort (consistent with its responsibilities as an ANSI-accredited standards-setting body) to expedite the completion of a stable, ballot-ready revision of J-STD-025 within the Commission's admittedly ambitious schedule of 180 days. In order to further expedite this standards-setting effort, TIA urges the Commission to be as specific as possible in defining any required modifications to J-STD-025. Representatives from the Commission should also participate in the standard's formulating group.

## **TABLE OF CONTENTS**

<b>Summary</b>	<b>i</b>
<b>I. Introduction</b>	<b>2</b>
<b>II. Implementing the Commission's Report and Order</b>	<b>7</b>
A. The Commission Should Authorize Subcommittee TR 45.2 to Modify J-STD-025 Consistent with the Commission's Report and Order	7
1. Overview of the TIA Standards-Setting Process	10
2. Standardization of the Commission's Report and Order	14
B. The Commission Should Establish a "Reasonable Time" for Compliance with its Report and Order	17
<b>III. Reasonably Available</b>	<b>20</b>
<b>IV. Proposed Modifications to J-STD-025</b>	<b>25</b>
A. DoJ/FBI's Proposed Modifications (the "Punch List")	26
1. Content of Subject-Initiated Conference Calls	26
2. Party Hold, Join, Drop on Conference Calls	28
3. Subject-Initiated Dialing and Signaling Information	30
4. In-Band and Out-of-Band Signaling	32
5. Timing Information	35
6. Surveillance Status Message	37
7. Continuity Check Tone	38
8. Feature Status Message	39
9. Dialed Digit Extraction	40
B. CDT's Proposed Modifications	43
1. Packet-Mode Communications	43
2. Location Information	48
<b>V. Conclusion</b>	<b>50</b>

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554

RECEIVED

DEC 14 1998

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

In the Matter of:

Communications Assistance for  
Law Enforcement Act

CC Docket No. 97-213  
FCC No. 98-282

To: The Commission

COMMENTS OF  
THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association ("TIA")<sup>1</sup> respectfully submits these comments on the Commission's recent *Further Notice of Proposed Rulemaking*<sup>2</sup> regarding the implementation of the Communications Assistance for Law Enforcement Act ("CALEA").<sup>3</sup> TIA appreciates the Commission's attention to the important issues raised in this proceeding and urges the Commission to act as swiftly as possible to resolve the remaining disputes regarding the industry CALEA standard for wireline, cellular and broadband PCS technologies -- J-STD-025.<sup>4</sup>

---

<sup>1</sup> TIA is a national, full-service trade association of over 900 small and large companies that provide communications and information technology products, materials, systems, distribution services and professional services in the United States and around the world. TIA is accredited by the American National Standards Institute ("ANSI") to issue standards for the industry.

<sup>2</sup> Further Notice of Proposed Rulemaking, *In the Matter of Communication Assistance for Law Enforcement Act*, FCC No. 98-282, CC Docket No. 97-213 (released on Nov. 5, 1998) ("Further Notice").

<sup>3</sup> Pub. L. 103-414, 108 Stat. 4279 (1994), *codified at* 47 U.S.C. §§ 1001 *et seq.*

<sup>4</sup> TIA & Alliance for Telecommunications Industry Solutions, J-STD-025, *Lawfully Authorized Electronic Surveillance*, Interim Standard (December 1997).

## I. Introduction

Although TIA does not agree with all of the tentative conclusions that the Commission reached in its *Further Notice*, TIA appreciates the Commission's careful attention to this proceeding and agrees with several of its preliminary decisions. In particular, TIA agrees with the Commission's proposed method for implementing its eventual Report and Order. As the Commission notes, Section 107(b)(5) "requires the Commission to provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under Section 103 during any transition period."<sup>5</sup> TIA respectfully urges the Commission to establish a transition period of no less than 36 months from June 30, 2000 (the Commission's deadline for the "core" J-STD-025) for carriers to comply with Commission's decision. This transition period would provide manufacturers approximately 24 months to design and develop the software and hardware modifications necessary to implement the Commission's order and would provide carriers roughly another 12 months to install and test these modifications.

TIA also strongly endorses the Commission's tentative conclusion to authorize TIA's Engineering Subcommittee TR 45.2 to undertake the task of modifying J-STD-025 to be consistent with the technical requirements the Commission ultimately adopts in this proceeding.<sup>6</sup> As discussed below, TIA agrees that TR 45.2 -- because of its unique expertise and resources -- is best qualified to issue a technical standard in the most efficient and expeditious manner. TIA will make every effort (consistent with its responsibilities as an ANSI-accredited standards-setting body)

---

<sup>5</sup> Further Notice, ¶ 29.

<sup>6</sup> *Id.*, ¶¶ 132-133.

to expedite the completion of a stable, ballot-ready revision of J-STD-025 within the Commission's admittedly ambitious schedule of 180 days.

TIA also agrees with the Commission's conclusion that it will not "reexamine any of the uncontested technical requirements of the J-STD-025 standard."<sup>7</sup> TIA views the relatively limited number of technical items at dispute in this proceeding (only eleven) as a testament to TR 45.2's careful and successful efforts to develop a reasonable standard that balances CALEA's competing interests in public safety, individual privacy and technological innovation.

TIA respectfully submits that the record in this proceeding already clearly establishes that J-STD-025 is not deficient and, hence, that no modification of the standard is necessary. The vast majority of comments received by the Commission in response to its previous *Public Notice*<sup>8</sup> on this matter support this conclusion.<sup>9</sup> Moreover, the few commenters who argue that J-STD-025

---

<sup>7</sup> *Id.*, ¶ 45.

<sup>8</sup> Public Notice, *In the Matter of Communication Assistance for Law Enforcement Act*, DA 98-762, CC Docket No. 97-213 (released on April 20, 1998).

<sup>9</sup> See Comments of AirTouch Communications, Inc. (May 20, 1998) ("AirTouch Comments"); Comments of the Ameritech Operating Companies, *et al.* (May 20, 1998) ("Ameritech Comments"); Comments of AT&T Corporation (May 20, 1998) ("AT&T Comments"); Comments of BellSouth Corporation, *et al.* (May 20, 1998); Comments of the Cellular Telecommunications Industry Association (May 20, 1998) ("CTIA Comments"); Comments of GTE Service Corporation, *et al.* (May 20, 1998); Comments of Nextel Communications, Inc. (May 20, 1998) ("Nextel Comments"); Comments of the Personal Communications Industry Association (May 20, 1998) ("PCIA Comments"); Comments of PrimeCo Personal Communications, L.P. (May 20, 1998); Comments of the Rural Cellular Association (June 12, 1998); Comments of SBC Communications, Inc. (May 20, 1998) ("SBC Comments"); Comments of Sprint Spectrum L.P. d/b/a Sprint PCS (May 20, 1998); Comments of the United States Telephone Association (May 20, 1998) ("USTA Comments"); Comments of US West, Inc. (May 20, 1998) ("US West Comments").

See also Reply Comments of AirTouch Communications, Inc. (June 12, 1998); Reply Comments of AT&T Corporation (June 12, 1998) ("AT&T Reply Comments"); Reply Comments of the Cellular Telecommunications Industry Association (June 12, 1998) ("CTIA Reply Comments"); Reply Comments of Nextel Communications Inc. (June 12, 1998) ("Nextel Reply Comments").  
(Continued ...)

is "deficient" take opposite views of the standard, agreeing with TIA in part and disagreeing in part. On the one hand, the Department of Justice ("DoJ") and the Federal Bureau of Investigation ("FBI") argue that industry must implement the FBI "punch list," but also defend J-STD-025's provisions on location tracking and packet data as consistent with CALEA.<sup>10</sup> On the other hand, the Center for Democracy and Technology ("CDT"), the Electronic Privacy Information Center ("EPIC"), the Electronic Frontier Foundation ("EFF"), the American Civil Liberties Union ("ACLU"), and a group including Americans for Tax Reform challenge the standard's treatment of location tracking and packet data, but otherwise oppose the DoJ/FBI Joint Petition and generally agree that J-STD-025 is not deficient.<sup>11</sup>

The broad support for J-STD-025 -- together with the fact that those challenging the standard attack it from opposite sides -- illustrates that the standard represents a reasonable interpretation of the requirements of CALEA. TIA urges the Commission to reach this conclusion. As discussed below, TIA continues to maintain that none of the proposed modifications to J-STD-025 are required by CALEA.

---

Comments); Reply Comments of PrimeCo Personal Communications, L.P. (June 12, 1998); Reply Comments of SBC Communications, Inc. (June 12, 1998) ("SBC Reply Comments"); Reply Comments of US West, Inc. (June 12, 1998) ("US West Reply Comments").

<sup>10</sup> See, e.g., Joint Comments of the Department of Justice and Federal Bureau of Investigation (May 20, 1998) ("DoJ/FBI Joint Comments"); Comments of New York City Police Department (May 20, 1998). See also Joint Petition for Expedited Rulemaking by the Department of Justice and Federal Bureau of Investigation (March 27, 1998) ("DoJ/FBI Joint Petition").

<sup>11</sup> See, e.g., Comments of the Center for Democracy and Technology (May 20, 1998) ("CDT Comments"); Joint Comments of the Electronic Privacy Information Center, the Electronic Frontier Foundation, and the American Civil Liberties Union (May 20, 1998) ("EPIC Comments"); Comments of Americans for Tax Reform, Center for Technology Policy, and Citizens for a Sound Economy (May 20, 1998). See also Petition for Rulemaking by the Center for Democracy and Technology (March 26, 1998) ("CDT Petition").

Indeed, the Commission already has reached this conclusion on four of the eleven items at issue in this proceeding. TIA endorses each of these conclusions. Specifically, TIA agrees with the Commission that location information, as provided by J-STD-025 (i.e., “cell site location at the beginning and termination of the call”), is consistent with the requirements of Section 103.<sup>12</sup> TIA also agrees with the Commission’s tentative conclusion that at least three of the FBI’s punch list items (surveillance status message,<sup>13</sup> continuity check tone<sup>14</sup> and feature status message<sup>15</sup>) exceed the scope of CALEA. As the Commission notes, although these features might be useful to law enforcement, they are neither call content nor call-identifying information and, hence, are not required by CALEA.

As for the other seven items on which the Commission has not yet reached a formal conclusion, TIA believes that the Commission should eventually decide that the proposed modifications are neither: i) required by Section 103 (i.e., neither call content nor call-identifying information), ii) “reasonably available” (if call-identifying information), nor iii) consistent with the five factors of Section 107(b).<sup>16</sup> For example, most of the in-band and out-of-band signaling

---

<sup>12</sup> Further Notice, ¶ 55.

<sup>13</sup> *Id.*, ¶ 109.

<sup>14</sup> *Id.*, ¶ 114.

<sup>15</sup> *Id.*, ¶ 120.

<sup>16</sup> As the Commission notes, Section 107(b) specifies five factors that the Commission must consider before establishing technical requirements to meet the assistance capability requirements of Section 103. These five factors require that the Commission’s eventual Report and Order must:

- (1) meet the assistance capability requirements of Section 103 by cost-effective methods;
- (2) protect the privacy and security of communications not authorized to be intercepted;

(Continued ...)

(“network signals”) sought by the FBI are neither call content nor call-identifying information required by Section 103 of CALEA. Moreover, even if certain network signals were viewed as call-identifying information, the extensive architectural changes necessary to capture and report such messages would dictate that this feature is neither “reasonably available” nor can be implemented in a “cost-effective method” that would “minimize the cost . . . on residential ratepayers.”

The proposed modification to J-STD-025’s treatment of packet-mode communications is of special concern to TIA’s members and TIA appreciates the Commission’s cautious approach to this item. As the Commission is no doubt aware, although packet-mode technologies are still evolving, the telecommunications network is rapidly transitioning to a packet-based architecture. It is imperative that the Commission not stifle the continued development of packet-mode technologies by imposing a solution that could require the redesign (or even abandonment) of certain technologies. Accordingly, TIA urges the Commission to preserve the flexible approach contained in J-STD-025. TIA also urges the Commission to be careful to preserve the distinction between telecommunications services (which are covered by CALEA) and information services (which are not) -- both of which employ packet-mode technologies. Perhaps the Commission should even consider excluding certain packet-mode technologies that are principally used to provide access to information-type services.

- 
- (3) minimize the cost of such compliance on residential ratepayers;
  - (4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and
  - (5) provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under Section 103 during any transition period.

CALEA, § 107(b); 47 U.S.C. § 1006(b).

As a final administrative note, TIA is aware that the Commission repeatedly has sought “rough” estimates of the price for developing the eleven items discussed in this proceeding.<sup>17</sup> Because of potential antitrust issues and the member companies’ extreme sensitivity in sharing this data (even with their industry association), TIA has decided not to collect such sensitive information from its members. However, it is TIA’s understanding that several manufacturers voluntarily have decided to provide this financial information, subject to a request for confidential treatment, so as not to deprive the Commission of access to information that the Commission appears to believe is highly relevant to its final decision.<sup>18</sup> These voluntary submissions should be treated with absolute confidentiality, pursuant to 47 C.F.R. § 0.459, and should not be placed in the Commission’s Public File. Such financial information -- even rough, preliminary estimates -- is highly confidential and the type of information that manufacturers ordinarily takes great lengths to keep secret from the public (especially its competitors in the highly competitive telecommunications equipment market). If an individual manufacturer’s request for confidentiality were to be denied, the Commission should return the materials without considering them, pursuant to 47 C.F.R. § 0.459(e).

## **II. Implementing the Commission’s Report and Order**

### **A. The Commission Should Authorize Subcommittee TR 45.2 to Modify J-STD-025 Consistent with the Commission’s Report and Order**

---

<sup>17</sup> See, e.g., Further Notice, Separate Statement of Commissioner Harold W. Furchtgott-Roth.

<sup>18</sup> TIA agrees with the Commission that such price estimates are an important factor in determining whether call-identifying information is “reasonably available.” Further Notice, ¶ 26. As discussed below, Congress included this qualification to ensure that carriers did not have to shoulder unreasonable costs and modify their systems to provide information that otherwise they had no business purpose for collecting.

However the Commission decides on the eleven items at issue in this proceeding, TIA strongly supports the Commission's conclusion to remand any technical modifications that might be required in J-STD-025 to TIA's Engineering Subcommittee TR 45.2 -- the technical subcommittee that drafted the standard. As the Commission noted, "the Subcommittee already has the experience and resources in place to resolve these issues more quickly [and] a Commission-based standard-setting activity would necessarily have to rely heavily on the Subcommittee to modify J-STD-025 in any event . . . ."<sup>19</sup>

Because of its unique membership of manufacturers and carriers, foreign and domestic representation, TR 45.2 represents the most talented collection of systems engineers from around the world. Remand to this Subcommittee would not only permit the development of a feasible technical standard in a relatively short period of time, it would also allow the Subcommittee to ensure that any modifications are harmonious with existing industry standards. Such standardization is critical to ensure network interoperability and preserve system reliability. As the Commission is aware, local exchange, cellular and broadband PCS providers' networks frequently intermix various manufacturers' telephone network elements. Thus, standards-based, compatible solutions are essential to ensure that such devices are fully interoperable.

Remand is also consistent with CALEA and with Commission precedent.<sup>20</sup> For

---

<sup>19</sup> Further Notice, ¶ 132. Note, in no way did TIA intend to imply in its previous comments that the Commission lacks the expertise to issue technical standards. Further Notice, ¶ 129. Instead, noting the Commission's large number of responsibilities and limited resources, TIA only meant to suggest that it would be more efficient for the Commission to remand any standardization work to TIA's standards-setting bodies.

<sup>20</sup> As TIA previously noted, while Section 107(b) permits the Commission to modify a deficient industry standard by rule, it does not require the Commission to do so. Indeed, the policies inherent in CALEA indicate a strong preference to defer to the telecommunications industry for the actual development of technical standards. *See, e.g.*, H.R. Rep. No. 103-827, at 19 (1994) ("House Report") ("The legislation provides that the telecommunications industry itself shall

(Continued ...)

these reasons, numerous commenters have supported the Commission's proposed approach.<sup>21</sup>

The Commission has proposed an ambitious schedule for TR 45.2 to complete its work -- 180 days. Although ambitious, TIA will make every effort (consistent with its responsibilities as an ANSI-accredited standards-setting body) to expedite the modification of J-STD-025. It is important to understand, however, that TIA is a member of, and has been accredited by, the American National Standards Institute to develop American National Standards for the telecommunications industry. Accordingly, TIA must operate its standards-developing bodies consistent with ANSI requirements.<sup>22</sup>

---

decide how to implement law enforcement's requirements. . . . This means that those whose competitive future depends on innovation will have a key role in interpreting the legislated requirements and finding ways to meet them without impeding the deployment of new technologies.”).

Remand to Subcommittee TR 45.2 also is consistent with the Commission's decision in recent proceedings to permit industry to issue and/or revise standards consistent with Commission determinations. *See, e.g.,* Report and Order, *Implementation of Section 551 of the Telecommunications Act of 1996; Video Programming Ratings*, CS Docket No. 97-55, FCC 98-35 (released on March 13, 1998); Report and Order, *Implementation of Section 304 of the Telecommunications Act of 1996; Commercial Availability of Navigation Devices*, CS Docket No. 97-80, FCC 98-116 (released on June 24, 1998).

<sup>21</sup> *See, e.g.,* AirTouch Comments, at 27; AT&T Comments, at 15-17; AT&T Reply Comments, at 3-7; CTIA Comments, at 18-22; CTIA Reply Comments, at 11-13; Nextel Comments, at 13; Nextel Reply Comments, at 8; PCIA Comments, at 6; PrimeCo Comments, at 22; SBC Comments, at 16; SBC Reply Comments, at 2; USTA Comments, Attachment at 7-9; US West Comments, at 31; US West Reply Comments, at 7-9.

<sup>22</sup> One of the most important of these requirements is that standards are available for public comment. As a result, non-TIA-members are strongly encouraged to participate in the standards-setting process. Such participation, as discussed below, may take the form of “liaison with appropriate Formulating Groups, participation in the open industry balloting of Standards Proposals, or active participation in Formulating Groups.” TIA Engineering Manual, § 3.2.4 (December 6, 1991) (attached as Appendix 1) (“Engineering Manual”).

## **1. Overview of the TIA Standards-Setting Process**

Because the Commission intends to entrust Subcommittee TR 45.2 with the important responsibility of modifying J-STD-025, as necessary, to implement the Commission's Report and Order, TIA here provides a brief overview of the standards-setting process.

First, any potential project is initiated by a "technical contribution" to one of TIA's Engineering Committees or Subcommittees from an individual requesting the creation of a new standard or technical document in a particular area of technology. TIA believes that such a contribution -- to authorize work to revise J-STD-025 -- is being prepared by TR 45.2 members for submission at the next TR 45.2 meeting this week in Florida. There, the contribution will be discussed and perhaps modified before being accepted by the Subcommittee.

Once the contribution is accepted, a Project Initiation Notice ("PIN") form is completed and submitted for approval to TIA. If TR 45.2 does submit a PIN after its December meeting, TIA will act to expeditiously approve the notice. After the project is approved, the "formulating group" (i.e., the Engineering Committee or Subcommittee that initiated the project) works to develop the technical parameters of the project. Assuming that a notice is submitted to TIA this month, a formulating group could be formed as soon as the next TR 45.2 plenary meeting in January.

There are two ways that an entity can participate in a formulating group. The first (and most common) way is for the entity to be a corporate member of TIA.<sup>23</sup> Part of the dues paid

---

<sup>23</sup> Engineering Manual, § 3.2.1.

by TIA member companies is used to support the standards-setting committees. However, “TIA Membership is not a pre-requisite to participation.”<sup>24</sup>

Non-member entities who have a “direct and material interest in a Standard” may participate in its formulating group by applying to TIA and paying the appropriate “non-member engineering participation fee.” Since non-member entities have not paid TIA dues, these fees are collected to help defray the costs of the standards-setting committees.<sup>25</sup> The fees for participating in each committee vary according to the level of activity within the respective committee and are assessed on an annual basis. Non-member entities that apply and pay the appropriate fee are fully entitled to participate within a formulating group -- including voting.

Non-member entities -- especially government representatives -- are always strongly encouraged to participate in TIA’s formulating groups.<sup>26</sup> Indeed, government participation is so strongly encouraged that “individuals from the federal, state and local government are allowed to participate at *no cost* as a ‘non-voting’ member of the various committees.”<sup>27</sup> In other words, without paying a fee, government representatives are entitled to attend meetings, receive materials, speak and submit contributions -- everything short of voting. Moreover, “[w]henver the federal government requests voting status on a TIA Standards Formulating Group, one such voting status

---

<sup>24</sup> *Id.*

<sup>25</sup> *Id.*, § 3.2.8

<sup>26</sup> *Id.*, § 3.2.4 (“TIA desires and encourages the active participation in its Standards-developing activities of all parties having a direct and material interest in its Standards, including U.S. federal, state and local government entities. . .”).

<sup>27</sup> TIA webpage on “How to Join TIA’s Engineering Committees,” <[www.tiaonline.org/standards/sfg/join.html](http://www.tiaonline.org/standards/sfg/join.html)> (attached as Appendix 2). *See also* Engineering Manual, § 3.2.4 (“[w]hen a government entity chooses to participate in a Formulating Group on a non-voting basis, *all fees are waived.*”) (emphasis added).

shall be granted without charge, with the understanding that the representative will represent the interests of the entire federal government.”<sup>28</sup>

Standards are developed through the submission of proposed text from members of the formulating group. This process can often span several months (if not years), as the members of the formulating group often will only meet for two days every month.<sup>29</sup> These submissions are debated and modified by the formulating groups during their monthly meetings. Text submissions generally are received and discussed in three stages. Stage 1 text describes the standard from the “User’s Perspective” and identifies the general, functional and physical requirements of the standard. Stage 2 text describes the standard from the “Network’s Perspective,” identifying the specific information provided by the standard. Stage 3 text describes the standard from the “Implementation Perspective” and is intended to assist engineers in the actual implementation of the standard -- establishing the specific protocols by which the messages that convey this information are to be constructed. Once a rough consensus is reached that the text for a given stage is stable and does not require extensive revision, that text is recognized by the formulating group as “baseline.” Note, identifying text as “baseline text” does not mean that the text cannot be revised; it simply means that there is sufficient consensus for the group to move onto the next stage.

When the proposed standard or technical document is near completion and the formulating group has reached consensus that it has a stable, baseline text for all three stages, the

---

<sup>28</sup> Engineering Manual, § 3.2.4. When more than one federal agency requests voting status (and are unable to agree upon consolidated representation), the additional agencies will be given such status, provided that the normal participation fees are paid by these agencies.

<sup>29</sup> It is important to realize that the engineers who sit on these formulating groups have a variety of important responsibilities. Many of the engineers who helped develop J-STD-025 also work on similar standards efforts for such issues as Enhanced 911 and number portability -- in addition to their work within their companies on developing new products.

group then proceeds to circulate the document for validation and verification ("V&V") review. The V&V review is intended to identify any unresolved issues and to establish consensus within the formulating group. It also permits a thorough editing to finalize the document for ballot. Every effort is made to resolve comments received. During this phase of the standards-making process, the draft of the document is not released to the general public. Once V&V is completed, the document is ready for ballot.

If the document is intended to be an American National Standard, the proposed draft must be circulated as a public ballot, also known as a "Standards Proposal" (SP) ballot. During the balloting period, *any interested party* may cast his/her vote. Indeed, it was a result of this public ballot (in which the FBI managed to organize considerable law enforcement response) that the industry standard was *twice* defeated as a potential ANSI standard (SP-3580 and SP-3580A).<sup>30</sup> A party can respond in three ways: affirmative, affirmative with comment or negative with comment. Every attempt is made to resolve comments received during balloting.

Standards can also be balloted as a TIA interim standard. "Interim Standards are issued where there is an urgent need for a standard, but the technology isn't stable enough for the issuance of an American National Standard."<sup>31</sup> Unlike an American National Standard, an Interim

---

<sup>30</sup> The Commission is correct that in the Spring of 1997, TR 45.2 first submitted the draft standard for balloting as a proposed ANSI standard (SP-3580). Further Notice, ¶ 12. However, the Commission is not correct that, after this ballot was defeated, "[t]he Subcommittee recommended that the revised standard be considered as a joint TIA/Committee T1 Interim Standard and reballoted under TIA procedures rather than ANSI's." Further Notice, ¶ 14. Actually, TR 45.2 -- concerned that law enforcement might prohibit the consensus necessary for adoption of the revised standard as an American National Standard -- proposed to ballot the revised standard *both* as a proposed American National Standard (SP-3580A) and as an Interim Standard (PN-4116). Both balloting procedures are consistent with ANSI procedures; the only difference is that an Interim Standard requires only the consensus of the formulating group.

<sup>31</sup> TIA Advisory Note No. 3 (May 24, 1993) (attached as Appendix 3).

Standard only requires the consensus of the formulating group for approval; it does not require the circulation of a Standards Proposal and its attendant public comments.<sup>32</sup> Interim standards must be reviewed by the formulating group annually and expire after three years (subject to one extension of a maximum of two years) unless the standard is in the public review process to become a TIA/American National Standard.

After the final draft of the document has obtained consensus (under either approach),<sup>33</sup> the document is forwarded with all its balloting information to a review group at TIA called the Telecommunications Standards Subcommittee (TSSC). If the document is intended to be a TIA/American National Standard, the same information is forwarded to the American National Standards Institute (ANSI) Board of Standards Review (BSR) with request for approval. The balloting information is then reviewed by TSSC and supporting documents are checked to see if TIA process and other requirements have been met. After this review and upon approval of the ANSI's BSR, the document is approved for publication as a TIA/ANSI Standard.

## **2. Standardization of the Commission's Report and Order**

Consistent with this process and its responsibilities as an ANSI-accredited organization, there are certain actions that TIA must take in complying with the Commission's remand. One such requirement is that TR 45.2 must place the revised standard out for public

---

<sup>32</sup> Engineering Manual, § 8.1. Because participation in formulating groups are open to any interested entity with a "direct and material interest in a Standard," any non-TIA-member entity that wishes to be able to vote on an Interim Standard should apply to TIA and pay the non-membership participation fee to become a member of the standard's formulating group.

<sup>33</sup> Note, consensus (under ANSI requirements) implies more than a simple majority but not complete unanimity.

comment and ballot (60 days for an ANSI standard) and, subsequently, must reconcile any comments received during the comment period (at least another 30 days) before submitting the final text to ANSI for adoption.

In order to complete a stable, revised J-STD-025 *and* complete this extensive (at least 3-5 months) balloting/reconciliation process within the Commission's 180-day deadline is probably not achievable. However, TIA does believe that TR 45.2, acting expeditiously, should be capable of completing its work in revising J-STD-025 and of having a stable document available for verification and validation within 180 days of the Commission's Report and Order. TIA would appreciate the Commission's clarification of whether this interpretation of its deadline is acceptable.

TIA would also appreciate the Commission's guidance on whether the revisions to J-STD-025 should be balloted as a TIA/American National Standard or as another Interim Standard. TR 45.2 is inclined to ballot the revisions as an American National Standard. However, as discussed above, balloting as a proposed ANSI standard would add procedures that would extend the balloting and approval process.

Finally, the Commission should appreciate that TIA will do everything in its power to expedite the standards process. However, because of its accreditation as a standards-setting body, TIA must remain neutral and cannot control or manage the actual work of the formulating group. Thus, if, in some unlikely event, the formulating group were unable to generate contributions or reach consensus on a text, TIA (other than encouraging the group) would not be able to take any action to break such an impasse.

Fortunately, TIA does not believe such a delay would occur. The members of TR 45.2 have expressed great appreciation of the important role that the Commission has assigned them and, as mentioned above, members of the Subcommittee are already preparing a request to initiate a

project number. TIA expects that as soon as the Commission's Report and Order is issued, members of the formulating group will have contributions to revise J-STD-025 ready for discussion and -- although the deadline is ambitious -- a stable, ballot-ready revision to J-STD-025 will be available by the Commission's deadline.

In order to expedite this standardization process, TIA respectfully would propose two recommendations to the Commission. First, TIA would strongly encourage representatives from the Commission's Office of Engineering and Technology to participate in the standards effort. Such representatives would be able to provide input from the Commission directly into the formulating group and, hopefully, would be able to avoid disputes that might emerge. Members of the privacy community and law enforcement are also strongly encouraged to participate.<sup>34</sup>

Second, the Commission should make every effort to make its decisions in this matter as specific as possible. A large reason for the continued disputes between law enforcement and industry over the punch list items is that law enforcement repeatedly has presented vague, broad requests from which it is difficult for industry to extract specific technical requirements.<sup>35</sup> The

---

<sup>34</sup> As discussed above, participation in a formulating group is open to any entity with a direct and material interest in a standard. To that extent, TIA respectfully takes exception with the suggestion by the EPIC, EFF and ACLU in their joint filing that the standards-setting process was "effectively closed to non-law enforcement and non-telecommunications industry participants." EPIC Comments, at 28. To the contrary, privacy groups are always welcome to participate in TIA's standards-setting process. Like any other party with a material interest in a standard, these groups were welcome to join the formulating group by applying to TIA and paying the appropriate "non-member engineering participation fee." Moreover, even without joining the formulating group, these groups could have commented on the standards when they were released for ANSI public ballot as at least one privacy group -- the Center for Democracy and Technology -- did. Perhaps the EPIC, EFF and ACLU previously were not aware that they could participate in the standards-setting process, but hopefully, now that they are, they will exercise that opportunity and will participate in the revision project.

<sup>35</sup> This pattern has continued in the Enhanced Surveillance Standard ("ESS") project, conducted at the request of the FBI "to develop and deploy additional features and capabilities, beyond those required by CALEA, in efforts to assist law enforcement agencies in conducting  
(Continued ...)

FBI's first "missing item" -- "All Content of Conferenced Calls" is an excellent example. In actuality, as the Commission is aware, J-STD-025 already provides law enforcement access to the contents of all conference calls to which the subscriber's terminal equipment is actually connected. The *only* conference-related call scenarios in which J-STD-025 does not provide access is when the subscriber places the other parties to the conference call on hold or drops off the line.<sup>36</sup> A general conclusion that "all content of conferenced calls" is required by CALEA is unlikely to provide much guidance in resolving this dispute. However, conclusions on specific call scenarios, much like the Commission has already suggested in its Further Notice,<sup>37</sup> would greatly assist the Subcommittee's work. Similarly, the Commission's guidance that "location information should be construed to mean cell site location at the beginning and termination of a call"<sup>38</sup> provides exactly the level of specificity that the formulating group needs to standardize that requirement.

**B. The Commission Should Establish a "Reasonable Time" for Compliance with its Report and Order**

As the Commission notes, Section 107(b)(5) "requires the Commission to provide a reasonable time and conditions for compliance with and the transition to any new standard,

---

lawfully-authorized electronic surveillance." Further Notice, ¶ 35. It has taken industry nearly a year to extract and refine the FBI's broad requests into anything remotely resembling a technical, functional requirement. Even despite this effort, the ESS text remains very much a work-in-progress.

<sup>36</sup> As discussed below, industry -- agreeing with privacy advocates -- maintain that, without the participation of the targeted subscriber's terminal equipment, the contents of the other parties' conversation is not subject to interception.

<sup>37</sup> See, e.g., Further Notice, ¶ 78.

<sup>38</sup> *Id.*, ¶ 55.

including defining the obligations of telecommunications carriers under Section 103 during any transition period.”<sup>39</sup>

As the Commission repeatedly has heard in related proceedings, manufacturers normally require at least 24 months from the existence of a stable technical standard to design, develop, test and make generally available the software and hardware necessary to comply with that standard.<sup>40</sup> Because of the technical difficulty of several of the punch list items (such as In-band and Out-of-Band Signaling and Surveillance Status Message), however, many manufacturers may require as much as 30-36 months to complete development of these features. Carriers, working with their manufacturers, usually require a subsequent twelve months to purchase, test, and install this equipment in all of their facilities.<sup>41</sup> Thus, TIA would recommend that the Commission establish a transition period that would give carriers no less than three years, from the completion of a revised J-STD-025, to deploy the equipment necessary to implement the Commission’s decision.

It is important to appreciate, however, that even once a revised J-STD-025 is available, most manufacturers will not be able to begin their design and development work until development and installation of the “core” J-STD-025 features is complete. Because of the resource constraints created by manufacturers’ extensive efforts to develop and deliver the core J-STD-025, manufacturers will be able to initiate work on the revised standard only when the engineering teams

---

<sup>39</sup> *Id.*, ¶ 29.

<sup>40</sup> Memorandum Opinion and Order, *In the Matter of Petition for the Extension of the Compliance Date under Section 107 of the Communications Assistance for Law Enforcement Act*, FCC No. 98-223, CC Docket No. 97-213 (released on September 11, 1998), ¶ 47. *See also* comments and petitions filed in that proceeding.

<sup>41</sup> *Id.*, ¶ 48.

currently devoted to the core J-STD-025 have completed their work and are able to turn to the revision.<sup>42</sup>

In addition, manufacturers' development cycles are planned several years in advance. For example, many manufacturers are already finalizing development plans for software and hardware releases that will not be generally available until 2000. Simply depending on whether a revised J-STD-025 is available before an individual manufacturer's "development window" closes could determine whether CALEA revisions will be included in the next release or will slip to the following release.

The Commission should also appreciate that, as is always the case with any feature development, there is a direct correlation between the difficulty of the project and the amount of time allocated to complete it. Thus, if industry were given a reasonable schedule (e.g., three years from June 30, 2000) to implement any revisions to J-STD-025, manufacturers and carriers would be able to allocate resources in a more efficient manner, working the revisions into their normal upgrade cycles. However, if the Commission were to establish an unreasonable transition schedule of less than three years from that date, manufacturers and carriers would have to disrupt their current development schedules and pull resources away from other products (with the attendant inefficiency of bringing the additional engineering teams "up to speed" on the new project) -- thus, raising the cost of compliance both for individual ratepayers and the government, meeting

---

<sup>42</sup> Wireline, cellular and broadband PCS manufacturers and carriers are working closely to comply with the Commission's extension of the compliance deadline for the "core" J-STD-025. In fact, partial solutions for most (if not all) platforms should be available by that date. However, simply because of the variety of architectures and systems employed by the industry, complete solutions consistent with the "core" J-STD-025 for all platforms may not be possible. As a result, additional individual petitions for extension may be necessary.

CALEA's capability requirements in a less cost-effective manner, and adversely affecting the provision of new technologies.<sup>43</sup>

Accordingly, TIA would respectfully suggest that the Commission establish a transition period of no less than 36 months from June 30, 2000 (the Commission's deadline for the "core" J-STD-025) for carriers to implement a revised J-STD-025. This transition period would provide manufacturers approximately 24 months to design and develop the software and hardware modifications necessary to implement the Commission's order and would provide carriers roughly another 12 months to install and test these modifications. The Commission should also recognize that because of the vagaries of development/installation schedules, in some individual cases additional extensions may be necessary.

### **III. "Reasonably Available"**

The Commission is correct to place great emphasis on Congress' qualification that only call-identifying information that is "reasonably available to the carrier" must be provided to law enforcement.<sup>44</sup> This limitation is consistent with the long-standing judicial principle that parties providing assistance to law enforcement cannot be asked to undertake burdens that are

---

<sup>43</sup> CALEA, §§ 107(b)(1),(3)&(4); 47 U.S.C. §§ 1006(b)(1),(3)&(4).

<sup>44</sup> CALEA, § 103(a)(2); 47 U.S.C. § 1002(a)(2). The Commission is also correct to look to the statutory definitions and court interpretations pertaining to "pen registers" and "trap and trace" devices for guidance. Further Notice, ¶ 27. In general, courts have been very restrictive of the type of information that can be obtained under such authorizations. *See, e.g., Brown v. Waddell*, 50 F.3d 285 (4th Cir. 1995). Indeed, CALEA specifically amended the pen register statute to limit the type of information collected under such authorizations: "LIMITATION -- A government agency authorized to install and use a pen register . . . shall use technology reasonably available to it that restricts the recording or decoding or electronic or other impulses to the dialing and signaling information utilized in call processing." CALEA, § 207(b); 18 U.S.C. § 3121(c).

unreasonable.<sup>45</sup> Thus, the Commission properly concludes that “before we can make a determination whether a specific technical requirement meets the mandates of Section 103’s assistance capability requirements, the Commission must determine whether the information to be provided to a LEA under Section 103(a)(2) is reasonably available to the carrier.”<sup>46</sup>

Unlike call content, where Congress spoke in absolute terms, the obligations of carriers and their equipment to provide call-identifying information are much more limited. A carrier must provide call-identifying information only if it is “reasonably available.” In addition, unlike the content of communications (which must be isolated “concurrently with their transmission to or from the subscriber’s equipment . . .”<sup>47</sup>), carriers are permitted greater latitude in deciding when to isolate call-identifying information -- either “before, during or immediately after the transmission of a wire or electronic communication . . .”<sup>48</sup> Finally, this category of information is narrowly defined by CALEA -- i.e., which phone number a party is calling from, which number it is calling to, whether the call is redirected, and the like.<sup>49</sup>

---

<sup>45</sup> See, e.g., *United States v. New York Telephone Co.*, 434 U.S. 159, 174 (1977) (“the power of federal courts to impose duties upon third parties is not without limit: unreasonable burdens may not be imposed.”); *In the Matter of the Application of the United States for an Order Authorizing the Installation of a Pen Register or Touch-Tone Decoder and a Termination Trap*, 610 F.2d 1148, 1155 (3rd Cir. 1979); *United States v. Mountain States Telephone and Telegraph Co.*, 616 F.2d 1122, 1132 (9th Cir. 1980). See also 18 U.S.C. § 2518(4) (“Any . . . person furnishing . . . facilities or technical assistance shall be compensated therefor by [law enforcement] for reasonable expenses incurred in providing such facilities or assistance.”).

<sup>46</sup> Further Notice, ¶ 25.

<sup>47</sup> CALEA, § 103(a)(1); 47 U.S.C. § 1002(a)(1).

<sup>48</sup> CALEA, § 103(a)(2); 47 U.S.C. § 1002(a)(2).

<sup>49</sup> CALEA, § 102(2); 47 U.S.C. § 1001(2). As the legislative history explains, for voice communications, call-identifying information “is typically the electronic pulses, audio tones, or signalling messages that identify *the numbers dialed* or otherwise transmitted for the purpose of routing calls through the communications carrier’s network.” House Report, at 21 (emphasis  
(Continued ...)

The FBI entirely ignores these critical limitations -- especially, the statutory provision that call-identifying information need only be provided to law enforcement if it is “reasonably available” to a telecommunications carrier. In its comments, the FBI states that “[a]lthough call-identifying information often will be accessed at a switch, the routing of calls may be controlled by network elements other than a switch, and call-identifying information may be ‘reasonably available’ elsewhere in the network.”<sup>50</sup> By this argument, the FBI appears to suggest that “reasonably available” means available *anywhere in any network*. Such an interpretation is inconsistent with the text and legislative history of CALEA.

First, certain call-identifying information may reside in a portion of the network not accessible to a carrier, such as a private branch exchange (“PBX”) or the network of another carrier with which the carrier subject to a wiretap order interconnects. It is plain that any such call-identifying information is not “reasonably available.” Indeed, CALEA explicitly excludes “equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers.”<sup>51</sup> Similarly, CALEA’s legislative history states: “[I]f an advanced intelligent network directs the communication to a different carrier, the subscriber’s carrier only has the responsibility . . . to ensure that law enforcement can identify the new service provider handling the communication.”<sup>52</sup>

---

added). The legislative history continues by defining such information in pen register investigations as “the *numbers* dialed from the facility that is the subject of the court order” and in trap and trace investigations as “the *originating number* of the facility that is the subject of the court order . . . .” *Id.* (emphasis added).

<sup>50</sup> DoJ/FBI Joint Comments, at 10 (citation omitted).

<sup>51</sup> CALEA, § 103(b)(2)(B); 47 U.S.C. § 1002(b)(2)(B). *See also* House Report, at 24 (“The bill does not cover private branch exchanges (PBX’s).”).

<sup>52</sup> House Report, at 22.

Second, even where particular information is in a part of the network accessible to a carrier, there may be no reason for the carrier's equipment to detect the information. For example, the FBI contends that post-cut-through dialed digits are call-identifying information. As discussed below, even if this information were call-identifying information to the originating carrier (which it is not), it is not "reasonably available" because the originating carrier has no reason to detect dialed digits that are not used for call routing and the manufacturers' switch designs do not contemplate their detection (since they are meaningless to the switch after the call is routed). Modifying these fundamental switch designs -- especially in wireless systems -- to enable the detection of such digits would be extraordinarily difficult and expensive.

Similarly, the FBI has sought an enormous variety of network-generated signaling (i.e., in-band and out-of-band signaling). Again, even if such signals were call-identifying information, they are not "reasonably available" because carriers have no purpose for detecting all of these signals (especially in one centralized location like the serving switch) and, hence, would have to make significant modifications to their equipment in order to do so.

The FBI contends that "the presence or absence of a 'business purpose' for collecting call-identifying information is simply irrelevant to whether the information is 'reasonably available' to the carrier."<sup>53</sup> In making this argument, the FBI apparently has forgotten that telecommunications carriers are in the business of providing telecommunications services to the public, not in the business of acquiring wiretap information for law enforcement. Congress explicitly recognized that if call-identifying "information is not reasonably available, the carrier does not have to modify its system to make it available."<sup>54</sup> It should go without saying that the

---

<sup>53</sup> DoJ/FBI Joint Comments, at 10.

<sup>54</sup> House Report, at 22.

reason that carriers build particular network capabilities is to serve the needs of their customers, and that these business purposes are directly relevant to whether particular information and capabilities are reasonably available to carriers.

In effect, the FBI seeks, self-servingly, to interpret the term “reasonably available” in a manner that reads it out of CALEA. The Commission should definitively reject this incorrect interpretation of a critical provision of CALEA. Congress included this important limitation regarding call-identifying information to avoid unjustified burdens on telecommunications carriers (and on the rate-paying public).

TIA would encourage the Commission to adopt J-STD-025’s conclusion that “information is reasonably available if the information is present at an Intercept Access Point (IAP) for call processing purposes.”<sup>55</sup> For most carriers, the IAP will be some centralized point like the subject’s serving switch or a Home Location Register (HLR).

The Commission is correct that because “carriers use a variety of system architectures and different types of equipment . . . reasonable availability is likely to vary from carrier to carrier.”<sup>56</sup> Indeed, because carriers frequently use equipment from different vendors, reasonable availability is likely to vary even within a carrier’s network (from one manufacturer’s equipment to another’s). Nevertheless, *all* of the call-identifying information sought by the FBI in this proceeding is not reasonably available to carriers -- because no carriers’ equipment currently collects the type of information sought by the FBI for call processing. For example, as already mentioned, no originating carrier captures (or has any reason to capture) post-cut-through digits;

---

<sup>55</sup> J-STD-025, § 4.2.1.

<sup>56</sup> Further Notice, ¶ 26. *See also* J-STD-025, § 4.2.1 (“The specific elements of call-identifying information that are reasonably available at an IAP may vary between different technologies and may change as technology evolves.”).

only the subsequent (terminating or intermediary) carrier has both the need and the ability to capture such digits. Thus, TIA would urge the Commission to reject the FBI's proposed modifications -- even for those items that might qualify as call-identifying information -- as not reasonably available.

#### **IV. Proposed Modifications to J-STD-025**

TIA strongly endorses the Commission's conclusion that it will not "reexamine any of the uncontested technical requirements of the J-STD-025 standard. Instead, we will make determinations only regarding whether each of the location and packet-mode provisions currently included within J-STD-025, and the nine punch list items that are currently not included, meet the assistance capability requirements of Section 103."<sup>57</sup> As the Commission notes "no party has raised any specific challenges to J-STD-025 other than with respect to these issues, and we have not been presented with any compelling reason to reexamine the entire standard."<sup>58</sup> The fact that so few items are at issue in this proceeding, as TIA and other commenters have noted, is a testament to industry's careful and successful efforts to develop a reasonable solution that balances the competing interests of law enforcement, privacy and technological innovation.<sup>59</sup> As discussed below, TIA continues to maintain that none of the modifications to J-STD-025 proposed by law enforcement and privacy groups are required by CALEA.

---

<sup>57</sup> Further Notice, ¶ 45.

<sup>58</sup> *Id.*

<sup>59</sup> *See, e.g.,* Ameritech Comments, at 3.

## **A. DoJ/FBI's Proposed Modifications (the "Punch List")**

### **1. Content of Subject-Initiated Conference Calls**

TIA agrees with the Commission's general statement that "the provision of the content of subject-initiated conference calls is a technical requirement that meets the assistance capability requirements of Section 103."<sup>60</sup> In fact, J-STD-025 already provides law enforcement with the content of subject-initiated conference calls; the *only* instance in which the standard does not provide law enforcement access is when the subject's terminal equipment (i.e., handset) is no longer connected to the call (either because the subject has dropped off the call or because he has placed the call on hold).

Industry, agreeing with the concerns raised by privacy groups, rejected the FBI's request as an exceptional expansion of law enforcement's ability to monitor communications.<sup>61</sup> As the CDT notes, "the FBI would require carriers to build the capacity to monitor all parties to a mutli-party call even after the subject of the intercept order is no longer participating in the call."<sup>62</sup> As TIA has previously discussed, the FBI's request would expand the scope of Title III's "facilities" doctrine.<sup>63</sup> Thus, to provide the contents of conference calls, even when the subject's

---

<sup>60</sup> Further Notice, ¶ 77.

<sup>61</sup> Even the FBI recognizes that the J-STD-025's treatment of conference calls "does not amount to a reduction in the information that has been available to law enforcement under POTS [Plain Old Telephone Service] . . . ." DoJ/FBI Joint Petition, at 30.

<sup>62</sup> CDT Comments, at 12.

<sup>63</sup> TIA Comments, at 34-38. As at least one court has noted, "'facilities' means the target telephones." *United States v. Tavarez*, 40 F.3d 1136, 1139 (10th Cir. 1994). See also 1 James G. Carr, *The Law of Electronic Surveillance* § 4.4(c)(2) (2d ed. 1988 Supp.).

telephone is not involved in the call, as the FBI requests, risks violating "the privacy and security of communications not authorized to be intercepted."<sup>64</sup>

Although the FBI's request is technically feasible, it would require a large re-development effort by most manufacturers. J-STD-025 provides that the call content channel ("CCC") follow the subscriber who is the target of the lawful authorization. Thus, when the subscriber places the conference on hold and takes a second call, the call content channel follows the subscriber to the new call, leaving the other parties on hold unmonitored.<sup>65</sup> In order to establish a separate call content channel for any parties on hold would require a substantial change to manufacturers' designs. In particular, the FBI's proposal would greatly complicate call-content-channel management -- requiring the carrier's equipment to provision a new call content channel whenever the subject places other parties on hold when the conference call was established with his "services," but not when the conference call was established on some other parties' "services." In order to have a call content channel immediately available for any held conversations, the carrier's equipment often will have to provision the additional call content channel prior to the conversation (and even so, there may be a slight delay before the additional call content channel is bridged to the held conversation).

Whatever action the Commission takes on this punch list item, TIA would urge the Commission to be very specific about which conference-related call scenarios carriers are required to assist law enforcement in monitoring -- as it has already started to do in its Further Notice.<sup>66</sup> As

---

<sup>64</sup> CALEA, § 107(b)(2); 47 U.S.C. § 1006(b)(2).

<sup>65</sup> Similarly, when the subscriber drops off of the call, the call content channel to the conference bridge is dropped.

<sup>66</sup> For example, the Commission concludes that "CALEA does not extend to conversations between a participant of the conference call other than the subject with whom the

(Continued ...)

discussed, J-STD-025 already provides law enforcement with access to the content of conference calls; access is not provided in only a few situations in which the subject's terminal equipment is not connected to the call. A general statement that "all content of subject-initiated conference calls" is required by CALEA is unlikely to provide sufficient guidance to resolve the technical and privacy disputes surrounding these contested call scenarios.

## **2. Party Hold, Join, Drop on Conference Calls**

As TIA explained in its previous comments, the information sought by the FBI under this punch list item is neither generated nor captured by a carrier's system in the manner in which the FBI would dictate. However, in order to address law enforcement's concerns, Subcommittee TR 45.2 added a new message to J-STD-025 -- the "Change" message -- to ensure that law enforcement is provided that information that is available to the carrier. TIA's members see no reason to modify J-STD-025 because the FBI would prefer a slightly different implementation.

For example, with respect to "party join," the J-STD-025's "Origination," "TerminationAttempt" and "Change" messages require that a carrier notify law enforcement whenever a new party joins a multi-party call either through initiation by the subject or through receipt of a call from a new party.<sup>67</sup> Similarly, J-STD-025's "Release" message requires notification to law enforcement whenever the switch detects that a party has "dropped" from the

---

participant speaks on an alternative line" and then provides a useful example. Further Notice, ¶ 78. TIA agrees with the Commission's conclusion that additional services invoked by held parties should not be subject to interception.

<sup>67</sup> See J-STD-025, § 5.4.4 (Change message); § 5.4.5 (Origination message); § 5.4.10 (TerminationAttempt message); Annex D.10.

call.<sup>68</sup> Although technically feasible, in order to provide this same information in the manner sought by the FBI would require considerable software coding to add the additional call processing traps and new messages necessary to report the information.

The *only* information that law enforcement might not obtain from J-STD-025's implementation is when a participant is placed on hold (or released from hold) by the intercept subject. However, as the Commission already realizes, changes to the parties on a call are not always detected by the switch.<sup>69</sup> This is particularly the case with hold information. As the Commission properly notes, "many telephone sets have a 'hold' button that does not signal the network -- thus, from the carrier's point of view, the call's status is unchanged."<sup>70</sup> Second, even when a change is detected, it is often likely that the switch will not have the specific identification information that the FBI has requested.

Thus, even if the Commission were to view "party hold" as call-identifying information (which TIA does not believe),<sup>71</sup> such information would not be reasonably available without modifications to most carriers' equipment. Moreover, in most cases -- even if a carrier's

---

<sup>68</sup> See J-STD-025, § 5.4.8.

<sup>69</sup> Further Notice, ¶ 86.

<sup>70</sup> *Id.* TIA also agrees with the Commission's observation that "[t]o the extent that customer premises equipment (CPE) is used to provide such features . . . party hold/join/drop information could not be reasonably made available to the LEA since no network signal would be generated." *Id.*

<sup>71</sup> TIA disagrees with the Commission's tentative conclusion that party hold information is call-identifying information because it "appears to identify . . . the temporary origin, temporary termination, or re-direction of a communication." Further Notice, ¶ 85. Whether a party is on hold or not is of no relevance to carriers (especially for purposes of routing a call). As discussed above, Congress meant for call-identifying information to be "the numbers dialed or otherwise transmitted for the purpose of routing calls through the telecommunications carrier's network." House Report, at 21.

equipment were modified -- no network signal would be generated for the carrier's equipment to detect. Finally, as the FBI concedes, party hold information is not information that law enforcement historically has received.<sup>72</sup>

For all of these reasons, TIA urges the Commission not to require an inefficient and unnecessary modification to J-STD-025. As TIA repeatedly has attempted to explain to the FBI, the standard already provides that information that is reasonably available to carriers.

### **3. Subject-Initiated Dialing and Signaling Information**

TIA disagrees with the Commission's tentative conclusion that "subject-initiated dialing and signaling information fits within the definition of call-identifying information contained in section 102(2)."<sup>73</sup> Actually, the information that the FBI requests (previously identified by the FBI punch list as "Feature Keys") has nothing to do with call-processing, but the method in which a subject has *enabled* a given feature.

In general, J-STD-025 already provides all of the relevant call-identifying information.<sup>74</sup> For example, when an intercept subject remotely enables call forwarding, there is no call-identifying information at that point because no call has actually been forwarded; the call-forwarding feature has only been enabled. However, as soon as a call is made to the subject's line,

---

<sup>72</sup> See DoJ/FBI Joint Petition, at 44.

<sup>73</sup> Further Notice, ¶ 91.

<sup>74</sup> As TIA has previously indicated, J-STD-025 provides information on all potentially-relevant call-identifying information relating to subject initiated dialing and signaling. TIA Comments, at 48-49. Through the "Change" (J-STD-025, § 5.4.4), "Redirection" (§ 5.4.7), "Origination" (§ 5.4.5), "TerminationAttempt" (§5.4.10), "Answer" (§ 5.4.1) and "Release" (§ 5.4.8) messages, J-STD-025 already identifies when a call is originated, forwarded (i.e., redirected), conferenced, merged, terminated, etc.

call forwarding will be invoked and -- pursuant to J-STD-025 -- the relevant redirection call-identifying information of the number to which the call is forwarded will be reported by the "Redirection" message.<sup>75</sup>

Similarly, the information that the FBI would appear to require with a separate "hook flash" message can be inferred from other messages already provided by J-STD-025. For example, in the case of three-way calling, the subject might hook flash to originate a new call leg. Under J-STD-025, a "CCClose" message may be generated to indicate that the subject has left the existing call leg to originate another call. An "Origination" message would be generated for each party called by the subject. When the new party added by the subject answers the call, an "Answer" message is generated and a "CCOpen" message may be generated. If the subject then causes the two legs to be conferenced, a "Change" message will be generated to indicate that the two legs have been merged.

The only additional information that law enforcement would receive under this punch list item is the actual keys pressed by the subject to enable the feature. It is unclear what benefit law enforcement would receive by having such information. In fact, in many cases the signaling information that the FBI seeks is redundant, misleading or even useless. (For example, what benefit does law enforcement derive from knowing that "Feature Key 12" has been depressed?) Even so, the identity of that key is not call-identifying information -- what events occur to the call because of the subject's action is the actual call-identifying information.

If the Commission were to determine that the feature keys used by a subject were call-identifying information, however, most manufacturers would have to make fairly substantial modifications to their equipment to capture and report such information. Most switches only detect

---

<sup>75</sup> J-STD-025, § 5.4.7.

the actual changes in calls (e.g., the destination or redirection of calls) -- information that J-STD-025 already provides. Most equipment does not identify the specific services that may have been invoked to cause that change.<sup>76</sup> That is why the J-STD-025 provides the information that it does, but does not identify the specific feature keys involved. To begin to capture the specific services involved would require carriers to make significant modifications to their equipment.

In addition, at least in the wireline environment, the large number of feature-specific keys that can be invoked only further complicates implementation. Indeed, the absence of a list of specific services for which carriers must provide notification has always complicated industry's evaluation of this item.<sup>77</sup> If the Commission were to require carriers to provide this punch list item, it should be very specific and enumerate the particular services for which law enforcement must receive notification

#### **4. In-Band and Out-of-Band Signaling**

Although TIA might agree that certain types of in-band and out-of-band signaling (i.e., "network signals") may constitute call-identifying information or call content, most of the enormously broad scope of signals sought by the FBI are *neither* call content nor call-identifying information. Moreover, capturing all of the signals that could be covered by the FBI's vague requirements (beyond that information already provided by J-STD-025) would require *extensive*

---

<sup>76</sup> In fact, in many instances there is no network signal for a carrier's equipment to detect. Thus, the Commission properly concludes that when "CPE is used to perform any of the functions described here, and no network signal is generated, that information will not be reasonably available to a carrier, and thus, should not be required to be provided." Further Notice, ¶ 92.

<sup>77</sup> For example, industry is fairly confident that law enforcement would not require notification of the subscriber's use of the "clock setting" service, although it is a feature that arguably would qualify as subject-initiated signaling.

architectural changes, indicating that this information is neither “reasonably available” nor can it be captured in a “cost-effective method” that would “minimize the cost . . . on residential ratepayers.” Indeed, following the December 3, 1997 technical meeting between industry and the FBI, industry engineers identified this item as one of the most technically difficult on the FBI’s punch list.<sup>78</sup>

There are literally *hundreds* of features supported by modern switches that provide some sort of in-band or out-of-band signaling within the scope of the FBI’s current request. In order to report this signaling, each of these features would require software modifications, affecting the entire system architecture. The FBI’s sweeping request for a wide variety of disparate and unidentified types of network signaling is emblematic of the approach the FBI has taken throughout the standards process. For this reason, if the Commission requires carriers to report network signals, TIA requests that the Commission be very specific in itemizing which particular signals are covered by its decision.

Moreover, many of the signals (in particular, the audible and visual indications) that the FBI is seeking are generated by peripheral equipment (in some cases the subject’s handset) without the knowledge of the serving switch. For example, in the frequent circumstance where a subscriber makes a long-distance call, the ring or busy signal for the called party is generated by the switch of a carrier other than the subscriber’s carrier.<sup>79</sup> If the Commission were to require this feature, it should clarify that carriers can provide notification only of those signals that are sent to the subject’s unit and that are generated by the serving switch. Signals generated from other

---

<sup>78</sup> Manufacturer’s Evaluation of Relative Feasibility of Punchlist Features (December 3, 1997) (attached as Appendix 4).

<sup>79</sup> The subscriber’s switch senses only whether the subscriber continues the call (which would likely happen if it is answered) or hangs up (which would likely happen if there is a busy signal or no answer). In any event, it is the subscriber’s action and not the remote audible signaling information that is detected by the local switch.

networked switches (i.e., the terminal switch), peripheral devices or the subject's handset cannot be interpreted or reported by a carrier.

In general, the industry standard already provides all of the relevant call-identifying information that a carrier could reasonably provide. For example, with respect to "alerting of incoming calls or messages," the "TerminationAttempt" message defined in J-STD-025 requires provision of a message at the time of each incoming call.<sup>80</sup> As for audible signals, J-STD-025 requires that the audible signaling information of which the local switch is aware should be provided over the call content channel. For subject-originated calls, the standard contemplates that the call content channel will be available to law enforcement as soon as the subject is "off-hook."<sup>81</sup> For calls received by the subject, the standard provides that "[l]oss of any portion (i.e., the beginning, middle, or end) of call content should not occur between call completion (answer) and call release."<sup>82</sup> Thus, if any audible signaling is available on the call content channel during the call, it will be provided to law enforcement. Indeed, the FBI recognizes that "[t]his information historically has been available to law enforcement on call content channels"<sup>83</sup> -- that is, it has been provided in just the manner that J-STD-025 requires. Even more important, the FBI has conceded that it is willing to accept access to audible signaling information on the call content channel, although it would "prefer" separate data messages regarding the signaling.<sup>84</sup>

---

<sup>80</sup> J-STD-025, § 5.4.10.

<sup>81</sup> *See id.*, Annex D.

<sup>82</sup> *Id.*, § 4.5.1.

<sup>83</sup> DoJ/FBI Joint Petition, at 46.

<sup>84</sup> Overhead Summary of FBI Comments/Clarifications of the Punchlist (December 5, 1997) ("Some user-perceived signals can be heard on the CCC and in those circumstances LE is  
(Continued ...)

It is important to remember, however, that most of these audible signals are not perceived by the local switch, but are generated further out in the network. To sense such signals would require a massive restructuring of system architectures and the installation of new equipment which would serve no network purpose -- *substantially* increasing the cost of telecommunications equipment (and ultimately the cost of service).

In sum, there is no basis for the Commission to find J-STD-025 deficient with respect to the provision of network-generated signaling information. J-STD-025 already provides law enforcement with access to that call-identifying information that is reasonably available to the serving switch. Most of the other signals sought by the FBI (in particular, audible and visual indications) are generated by remote networks or peripheral equipment without any knowledge of the local switch. However, if the Commission were to determine that some of this information is call-identifying *and* is reasonably available, the Commission should enumerate the specific signals that must be reported. Otherwise, the FBI's current request would require manufacturers to make modifications in potentially hundreds of different features.

## **5. Timing Information**

Although TIA does not agree with the Commission's tentative conclusion that "time stamp information fits within the definition of call-identifying information,"<sup>85</sup> industry has never opposed the inclusion of a timing provision within J-STD-025. Instead, industry's only objection has been with the unreasonable technical requirements proposed by the FBI. Specifically, the FBI's

---

willing to accept access to the CCC as opposed to separate signals on the CDC, but would prefer a separate message on the CDC") (attached as Appendix 5).

<sup>85</sup> Further Notice, ¶ 104.

original request for delivery of call-identifying information within 500 milliseconds was simply impossible to implement.

As the Commission notes, CALEA provides that “carriers must ‘expeditiously’ isolate and enable the government to access call-identifying information ‘before, during, or immediately after the transmission of a wire and electronic communication . . . and in a manner that allows it to be associated with the communication to which it pertains.’”<sup>86</sup> Rather than adopt the FBI’s original request, J-STD-025 incorporated this statutory requirement -- requiring that the “Call-Identifying Information IAP (IDIAP) . . . provid[e] expeditious access to the reasonably available call-identifying information” and contemplating that information would be provided to law enforcement as soon as it is generated.<sup>87</sup> As manufacturers have repeatedly explained to the FBI, they have no plans to intentionally delay (or “buffer”) delivery of such information; indeed, to build in a delay would require additional development.

While manufacturers would prefer to maintain the standard’s “expeditious access” requirement, they are willing to replace that provision with a specific amount of time, so long as that time is reasonable and consistent with current system architectures.

The FBI’s more recent request for 3 seconds with a probability of 99 percent, although more reasonable, is not a requirement that most manufacturers could guarantee. Assuming that the timing requirement applies to the time between detection of the event by the Delivery Function and the actual sending of the message from the Delivery Function toward law enforcement’s Collection Function (i.e., to begin transmitting), 8 seconds with 95 percent probability seems more feasible. Even this timing requirement might not be achievable in all

---

<sup>86</sup> *Id.* (quoting CALEA, § 103(a)(2); 47 U.S.C. § 1002(a)(2)).

<sup>87</sup> J-STD-025, § 4.4.

networks, in all circumstances and would depend upon such factors as switch load and carrier network configurations. For example, under extremely heavy loads (like on Mother's Day) such timing requirements could not be satisfied. Obviously, this timing requirement would also depend on the availability of call data channels (CDCs).

As for the FBI's requirement that messages be stamped with a time stamp accurate to 100 milliseconds, there is some confusion about the basis of this accuracy (i.e., accurate to what?). However, if agreement can be reached on some common basis (e.g., arrival at the Delivery Function), most manufacturers seem able to satisfy a level of accuracy near 200 milliseconds.

#### **6. Surveillance Status Message**

TIA completely agrees with the Commission's conclusion that the "surveillance status punch list item is not an assistance capability requirement under Section 103."<sup>88</sup> As the Commission properly notes, the surveillance status message -- although perhaps useful to law enforcement -- is not "call-identifying information as defined by CALEA, since the information such a feature would provide is unrelated to any call . . ." and is not "required under Section 103(a)(1), since it is not necessary to intercept either wire or electronic communications carried on a carrier's system."<sup>89</sup> In fact, the FBI, recognizing that no specific statutory basis existed for its request, was forced to offer a novel interpretation of Section 103's "shall ensure" language that the Commission correctly discounted. As the Commission properly concluded, "[w]e interpret the

---

<sup>88</sup> Further Notice, ¶ 110.

<sup>89</sup> *Id.*, ¶ 109.

plain language of the statute to mandate compliance with the capability requirements of Section 103(a), but not to require that such capability be proven or verified on a continual basis.”<sup>90</sup>

In addition to the complete absence of any statutory basis, the FBI’s request would be extremely difficult and costly to implement. In the wireless context, for example, it would require significant modifications to system architecture to verify electronically that every relevant mobile switch (and every other piece of network equipment containing intercept-related data) is operational and properly configured. No infrastructure is currently in place to permit carriers to poll network equipment in that manner. As a result, the FBI’s request is one of the more technically difficult items on their punch list. The development and implementation of such a capability would be costly and complex, especially as carriers can manually check such equipment to ensure their operation. Accordingly, to mandate the automated system requested by the FBI would clearly violate Section 107(b)’s requirements to implement CALEA in “cost-efficient methods” and to “minimize the cost . . . to residential ratepayers.”<sup>91</sup>

## **7. Continuity Check Tone**

Similarly, TIA agrees with the Commission that, although a continuity check tone might be useful to law enforcement, “this technical requirement is not necessary to meet the mandates of Section 103(a).”<sup>92</sup> As with the surveillance status message, TIA agrees with the Commission that a continuity check tone is neither call-identifying information nor call content, and that Section 103’s “shall ensure” language does not impose an additional obligation for carriers to

---

<sup>90</sup> *Id.*

<sup>91</sup> CALEA, § 107(b)(1)&(3); 47 U.S.C. § 1006(b)(1)&(3).

<sup>92</sup> Further Notice, ¶ 114.

“provide or verif[y] on a continual basis” their compliance with CALEA’s assistance capability requirements.<sup>93</sup>

In order to provide this feature, carriers would have to make unnecessary modifications to their systems, in many instances having to purchase additional hardware (for example, a dedicated C-tone generator for each trunk) that otherwise they would have no business purpose for obtaining. At present, switches use C-tone only within the local loop.

### **8. Feature Status Message**

TIA also agrees with the Commission’s conclusion that although “feature status messages could be useful to a LEA, . . . provision of these messages from a carrier to a LEA is not required to meet the mandates of Section 103(a).”<sup>94</sup> As with the surveillance status message and continuity check tone, TIA agrees that a feature status message is neither call-identifying information nor call content, and that Section 103’s “shall ensure” language “does not require carriers to implement any specific quality control capabilities to assist law enforcement.”<sup>95</sup>

Moreover, like surveillance status message, the FBI’s feature status message is one of the most technically difficult features on the punch list. Implementation of this feature would require manufacturers to build intercept capability into a number of different system platforms -- like the Home Location Register -- and reconfigure entire customer service databases and other operating software to provide automatic messaging to law enforcement -- a capability that is not even remotely supported by the present design of these systems. In addition, there is the

---

<sup>93</sup> *Id.*

<sup>94</sup> *Id.*, ¶ 121.

<sup>95</sup> *Id.*

complication of features provided by third-party peripheral devices. Carriers might be forced to create interconnections to contractors and other service providers who manage such devices. Given that this information is currently gathered through periodic, manual verification of subscriber records (subject to a subpoena),<sup>96</sup> provision of this automated feature would clearly violate the requirement to implement CALEA in “cost-efficient methods” and to “minimize the cost . . . to residential ratepayers.”<sup>97</sup>

## **9. Dialed Digit Extraction**

TIA disagrees with the Commission’s tentative conclusion that “post-cut-through digits representing all telephone numbers needed to route a call, for example, from the subscriber’s telephone through its LEC, then through IXC and other networks, and ultimately to the intended party are call-identifying information.”<sup>98</sup> From the originating carrier’s perspective, post-cut-through digits are not call-identifying information. *The originating carrier has no purpose to intercept such digits for call processing purposes.* For the originating carrier, these digits are simply call content.<sup>99</sup> The originating carrier has no method of identifying whether such digits are being used for call routing or other purposes (such as responses to an automatic queuing system, a PIN or a credit card number). Post-cut-through digits are only call-identifying information for a

---

<sup>96</sup> CDT Petition, at 14.

<sup>97</sup> CALEA, § 107(b)(1)&(3); 47 U.S.C. § 1006(b)(1)&(3).

<sup>98</sup> Further Notice, ¶ 128.

<sup>99</sup> Indeed, the FBI previously recognized this fact. During one of the legal summits held to resolve legal disputes between industry and law enforcement during the creation of J-STD-025, the FBI indicated that law enforcement would simply obtain a Title III order so that it could have access to the call content channel and extract such information with its own DTMF receivers.

subsequent carrier who uses the digits for call processing (and from whom law enforcement can obtain the information).<sup>100</sup>

Because the originating carrier has no purpose for intercepting these digits, provision of post-cut-through digits (like all of the FBI's requirements) is not "reasonably available" in current networks. First, in many wireless architectures, tone decoders are not even used for normal call processing. Instead, numbers are transmitted only after the subject presses the "send" key. Thus, to collect post-cut-through digits would require major software re-architecture and significant changes in engineering and capacity guidelines for the mobile switch center (to accommodate the additional tone decoder hardware).

Second, even in wireline architectures, the DTMF tone receiver is only connected until the call is completed (i.e., "cut through"). Once the call is cut through, the tone receiver is available for use on another call. Because tone receivers can be recycled in this way, manufacturers build switches with a number of tone receivers that is far lower than the number of simultaneous calls that a switch can support. However, under the FBI's requirement, digital tone receivers would have to be dedicated to each intercepted call for the entire duration of the call. These tone receivers

---

<sup>100</sup> In fact, it was Congress' explicit intent that law enforcement access call-identifying information only from the carrier for whom such information is reasonably available, even if that meant that law enforcement might have to go to several different carriers to obtain all such information about a call. For example, in the context of forwarded calls, the legislative history explains that

"If, for example, a forwarded call reaches the system of the subscriber's carrier, that carrier is responsible for isolating the communication for interception purposes. However, if an advanced intelligent network directs the communication to a different carrier, the subscriber's carrier only has the responsibility . . . to ensure that law enforcement can identify the new service provider handling the communication."

House Report, at 22.

could not be shared for any other switching functions. Thus, implementation of this requirement would not only require changes in the software controlling switching call logic, but extensive engineering modifications would have to be made to the switch to accommodate the additional tone receivers that would have to be dedicated to CALEA.

The Commission should remember that the originating carrier has no call processing or other business purpose for developing this expensive capability; this cost would only be incurred for purposes of CALEA. Given that the post-cut-through digits can be obtained from subsequent carriers (for whom the digits are call-identifying information), mandating this requirement would clearly violate the requirement to implement CALEA in “cost-efficient methods” and to “minimize the cost . . . to residential ratepayers.”<sup>101</sup> Recognizing the “inordinate expense” to design, build and incorporate this feature into the telephone network infrastructure, the Commission suggested “the possibility that there may be newly available, less expensive solutions for this feature.”<sup>102</sup> It is TIA’s understanding (although it has been unable to confirm this fact) that the solution mentioned by the Commission is no longer being developed by that manufacturer. The Commission may wish to confirm this fact.

Moreover, the delivery of post-cut-through digits pursuant to a pen register order would not protect “the privacy and security of . . . call-identifying information not authorized to be intercepted . . . .”<sup>103</sup> As the Commission is aware, post-cut-through digits can include all sorts of sensitive information (credit card numbers, bank account numbers). TIA’s manufacturers are not aware of any reasonably available method by which “call-identifying information can be

---

<sup>101</sup> CALEA, § 107(b)(1)&(3); 47 U.S.C. § 1006(b)(1)&(3).

<sup>102</sup> Further Notice, ¶ 128.

<sup>103</sup> CALEA, § 107(b)(2); 47 U.S.C. § 1006(b)(2).

distinguished from digits dialed to perform other functions (e.g., to input a credit card number or to access information services after the call reaches its final destination in the PSTN)."<sup>104</sup> As mentioned above, the originating switch has no method of identifying whether such digits are being used for call routing or other purposes.

## **B. CDT's Proposed Modifications**

### **1. Packet-Mode Communications**

TIA endorses the cautious approach taken by the Commission in establishing technical requirements for packet-mode telecommunications services.<sup>105</sup> As the Commission properly notes, "packet-mode technology is rapidly changing, and . . . different technologies may require differing CALEA solutions."<sup>106</sup>

In many ways, packet-switching technology (particularly in the wireless environment) is still in its infancy. No one knows how the technology will evolve or in what new capacities it will be employed. Because of the increased capacities they can provide, packet-mode technologies are being employed for a variety of different services, in many cases replacing legacy,

---

<sup>104</sup> Further Notice, ¶ 128.

<sup>105</sup> TIA also agrees with the Commission's emphasis on the distinction that packet-switching technology is subject to CALEA *only* to the extent it is used to provide telecommunications services, and not for information services. Further Notice, ¶ 63. It is important that CALEA's requirements not expand to encompass services (i.e., information services) that Congress clearly intended to exclude, simply because these services employ packet-mode technologies that are also employed for communications services. TIA would urge the Commission, either in this or a subsequent rulemaking, to identify which services qualify as information services and which as telecommunications services. The Commission also should consider excluding certain packet-mode technologies (like Cellular Digital Packet Data (CDPD)) that are principally used to provide access to information-type services.

<sup>106</sup> Further Notice, ¶ 64.

circuit-mode technologies. The number of carriers beginning to offer voice-over-IP telephony services is a perfect example of this transition. As the Commission noted, J-STD-025 identified at least eight different categories of telecommunications services employing packet-mode technologies, and that list is far from complete.<sup>107</sup> Which technologies will become the technologies of the network of the future is still unclear.

Specifically because of the variety of different packet-mode technologies and the inability to predict how such technologies might develop, TR 45.2 consciously choose to preserve the flexibility of carriers to comply with CALEA's requirements through different methods. Even between the various platforms offered by a single manufacturer, the solutions for collecting packet-mode information may differ dramatically by platform. For example, one platform (employing one type of packet-mode technology) may have relatively easy access to the address portions of packet communications, while a different platform (employing a different technology) would only be able to obtain such information through major redesign of its architecture.

It is imperative that the Commission not stifle the continued development of packet-mode technologies by imposing a single solution that could require the redesign (or even abandonment) of certain technologies.<sup>108</sup> Accordingly, TIA strongly urges the Commission to preserve the flexible approach contained in J-STD-025.

The CDT Comments state that the provision of J-STD-025 permitting the delivery of a complete packet stream to law enforcement is based "[o]n the untested assumption that it is not

---

<sup>107</sup> Further Notice, ¶ 64 & n. 121.

<sup>108</sup> As the Commission is aware, one of the factors that it must consider under Section 107(b) is "the policy of the United States to encourage the provision of new technologies and services to the public." CALEA, § 107(b)(4); 47 U.S.C. § 1006(b)(4). TIA can state without hesitation that the technical mandate proposed by CDT and the other privacy groups -- no matter how laudable -- will have a dramatic impact on the development of new packet-mode technologies.

feasible to provide signaling information separate from content in a packet switching environment.”<sup>109</sup> Furthermore, CDT suggests that available technology permits separation of signaling information from packet content in X.25, Transmission Control Protocol/Internet Protocol (“TCP/IP”), and Asynchronous Transfer Mode (“ATM”) communications.<sup>110</sup> These contentions are not accurate.

It is not an “untested assumption” that it is difficult for telecommunications carriers to separate signaling information from content in packet-switched communications.<sup>111</sup> The relative ease of separating such information may differ from technology to technology; however, most existing telecommunications networks do not have the technology to provide this capability and most carriers do not have a business purpose for developing such capability. For that reason, separation of call-identifying information from the remainder of a packet is not reasonably available and would require the modification of carriers’ equipment.

An added complexity is the “layered” structure of most packet-mode technologies. All packet data protocols, including X.25, TCP/IP and ATM, are based upon the layered protocol stack structure defined by the International Organization for Standardization and the International

---

<sup>109</sup> CDT Comments, at 34.

<sup>110</sup> *See id.*, at 36-37.

<sup>111</sup> In its Further Notice, the Commission seeks comments on “what constitutes the equivalent of ‘call-identifying information’ for packet-mode telecommunications services . . . .” Further Notice, ¶ 65. Unfortunately, the answer differs widely based on the technology being employed. For example, for Internet-protocol (IP)-based services, the equivalent of call-identifying information probably could consist of the “source” IP address and the “destination” IP address of each packet. From these addresses, law enforcement should be able to identify the “origin, direction, destination or termination of each communication generated or received by a subscriber . . . .” CALEA, § 102(2); 47 U.S.C. § 1001(2). However, for certain X.25 services there might be nothing that would equate to call-identifying information, and in other X.25 services the equivalent of call-identifying information might consist of the call control packets that establish and take down the virtual call.

Telecommunication Union. In a layered protocol, each layer views the layer above it as content. The content for the current layer, plus its routing information (the header), becomes the content portion for the next lower layer. A telecommunications carrier transporting packet data is often responsible for providing hardware and software support only for the physical layer, and does not have any reason to segregate higher-layer content from higher-layer routing information. It is important that the Commission clarify that a carrier is responsible -- at most -- for providing that layer of information that it reads and normally uses in routing packets.

Even this is a major undertaking, however. To extract packet routing information, two basic steps must be completed. First, packets of interest must be identified and captured. *Identification of particular packets for the purpose of extracting call-identifying information presents technical challenges that most carriers are not currently capable of meeting.* In a stream of bits riding across a circuit, the system must be able to recognize the sequence of bits that delineate the start of a packet that should be intercepted. This can require that the system "watch" all circuits, all the time, looking for specific packets. Such a requirement would be *very* processor-intensive, adversely impacting the other network packet functions that the processors perform.

Moreover, even once packets have been identified, the relevant information still must be extracted. The process of extracting "call-identifying" equivalent information from a packet stream is very difficult. In many packet-mode technologies, what the FBI might consider "call-identifying" information is embedded in the packet. Thus, to require a carrier to extract such information would require a carrier to break into the packet and separate that information from the remaining contents of the packet -- something that most systems do not currently do.

An added level of difficulty exists in extracting header information from content in a layered protocol stack. To obtain routing information at the level sought by law enforcement, a

carrier might need to extract headers from several layers. At each layer, the system must not only recognize the beginning and end of each packet, but must recognize the protocol being used so that it can separate the header from the content. This analysis would require technology that is not now available in most carrier networks.

This is not to say, however, that packet-mode technologies might not evolve such that the separation of "call-identifying" information from a packet may become easier. For some applications, such separation may already be relatively simple. Indeed, J-STD-025 permits carriers to employ such a solution if its technology provides for the separation of source and destination information. However, because of the continued evolution of packet-mode communications (and its variety of different applications), it is important that the Commission not adopt a technical requirement that might serve as a straight-jacket to such development. Accordingly, TIA strongly encourages the Commission to preserve the flexibility contained in J-STD-025.

Alternatively, the Commission might consider establishing a separate standard-setting effort within TIA for packet-mode communications. Such an effort would require a compliance schedule and technical requirements independent from the punch list features addressed in this proceeding. If the Commission were to consider authorizing such an effort, TIA would urge the Commission to consider a separate rulemaking to identify specific packet-mode technologies for which CALEA compliance is not required and, otherwise, to provide guidance to TIA's standards-setting efforts.<sup>112</sup> Given the rapid evolution and obsolescence of packet-mode technologies, a separate standards-setting effort may be the most effective method for implementing CALEA.

---

<sup>112</sup> For example, some manufacturers have expressed interest in exempting CDPD traffic as: 1) a technology that is being replaced in the industry by newer and more widely accepted data technologies (and whose imminent obsolescence is expected), 2) as a technology used by a small fraction of users and principally for access to information-type services, and 3) a technology  
(Continued ...)

## 2. Location Information

Finally, TIA agrees with the Commission that location information, as provided by J-STD-025, is consistent with the requirements of Section 103. To the extent that J-STD-025's provisions are viewed as unclear, TIA welcomes the Commission's proposed clarification that "location information should be construed to mean cell site location at the beginning and termination of the call"<sup>113</sup> -- a clarification which is completely consistent with J-STD-025.

Although the Center for Democracy and Technology is correct that Congress wanted to avoid turning wireless handsets into tracking devices,<sup>114</sup> TIA believes that J-STD-025 reflects the appropriate balance between law enforcement interests and privacy concerns.

J-STD-025 intentionally does not incorporate law enforcement's original, much broader request that carriers continuously track the movement of a wireless phone (whether it was being used to place a call or not). Subcommittee TR 45.2 rejected that request as violating CALEA's privacy provisions. Instead, the standard only requires that a carrier provide the location (by cell site) of a wireless phone at the beginning and termination of a call, information roughly analogous to that which Congress has authorized law enforcement to receive -- the location that "may be determined from the telephone number."<sup>115</sup> As the Commission notes, "in the wireline environment . . . LEAs have been able to obtain location information routinely from the telephone

---

whose design makes interception particularly difficult to implement without substantial system re-design.

<sup>113</sup> Further Notice, ¶ 55.

<sup>114</sup> CDT Comments, at i. *See, e.g.*, CALEA, § 103(a)(2); 47 U.S.C. § 1002(a)(2) ("call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number.").

<sup>115</sup> *See, e.g.*, CALEA, § 103(a)(2); 47 U.S.C. § 1002(a)(2).

number because the telephone number corresponds with [a] location” and “the equivalent location information in the wireless (cellular or broadband PCS) environment appears to be the cell site. . .

”<sup>116</sup>

In general, cell site information at the beginning and end of a call is reasonably available in most wireless networks.<sup>117</sup> However, the Commission should be aware that in some systems, cell site location may not be available at the termination of a call (depending on whether the subject roams into an area served by a different switch than originated the call). The Commission should also be aware that location information in a level of granularity beyond the cell site handling the call is not reasonably available in most systems.

Accordingly, TIA would agree with the Commission’s proposed clarification to J-STD-025 that “location information should be construed to mean cell site location at the beginning and termination of the call,”<sup>118</sup> so long as the Commission recognizes that in some instances provision of cell site location (at least at the termination of a call) may not be possible.

---

<sup>116</sup> Further Notice, ¶ 53 & n. 100.

<sup>117</sup> In its Further Notice, the Commission notes that “wireless carriers will be required to have a location information capability as part of their E911 obligations.” Further Notice, ¶ 56. Although there are some general similarities, the Commission should be aware that for many manufacturers the development of E911 location tracking and CALEA location information is distinctly separate. Location, for J-STD-025 purposes, will require different software and cannot utilize E911 capabilities.

Nevertheless, TIA does agree that E911 obligations can be used as a rough measure of whether certain technologies -- other than cellular, wireline and broadband PCS -- are able to provide location information under CALEA. As the Commission is aware, several technologies that are not specifically addressed in this rulemaking (such as paging) were specifically exempted from E911 requirements and TIA would urge that, for the same reasons, these technologies should be excluded from providing location information under CALEA.

<sup>118</sup> Further Notice, ¶ 55.

## V. Conclusion

For the reasons set out above, the Commission should conclude that J-STD-025 is not "deficient" and should deny the modifications proposed by the FBI and the Center for Democracy and Technology. However, if the Commission does conclude that J-STD-025 is "deficient" in any respect, it should not adopt specific technical standards; instead, as it has proposed, the Commission should indicate the areas of deficiency -- with as much detail and specificity as possible -- and return to TIA the task of setting such standards as may be necessary to remedy these deficiencies. The Commission should also provide the "reasonable time" specified in CALEA for transition to any new Commission-mandated standard. TIA suggests that at least three years from June 30, 2000 (the Commission's deadline for the "core" J-STD-025) should provide manufacturers with sufficient time to design and develop the software and hardware upgrades necessary to implement these revisions and also provide carriers with sufficient time to install these upgrades.

Respectfully submitted,

  
**Telecommunications Industry Association**

Stewart A. Baker  
Thomas M. Barba  
L. Benjamin Ederington  
**Steptoe & Johnson LLP**  
1330 Connecticut Avenue, N.W.  
Washington, D.C. 20036  
(202) 429-3000

Grant Seiffert  
Vice President, Government Relations  
Matthew J. Flanigan  
President  
1300 Pennsylvania Avenue, N.W.  
Suite 350  
Washington, DC 20004  
(202) 383-1483

December 14, 1998

## **APPENDICES**

- Appendix 1:** TIA Engineering Manual (December 6, 1991)
- Appendix 2:** “How to Join TIA’s Engineering Committees,” <[www.tiaonline.org/standards/sfg/join.html](http://www.tiaonline.org/standards/sfg/join.html)>
- Appendix 3:** TIA Advisory Note No. 3 (May 24, 1993)
- Appendix 4:** Manufacturer’s Evaluation of Relative Feasibility of Punchlist Features (December 3, 1997)
- Appendix 5:** Overhead Summary of FBI Comments/Clarifications of the Punchlist (December 5, 1997)